DEPARTMENTAL GENERAL ORDER

~~I-20~~: REMOTE AND MOBILE CAMERAS (RMC)

Effective Date:
Coordinator: Information Technology Unit, Bureau of Services Division

The Oakland Police Department (OPD) uses technology to more effectively promote public safety; OPD also strives to institute policies that promote accountability and transparency. This policy provides guidance and procedure for the use, documentation, and auditing of live-stream mobile cameras.

All data, whether sound, image, or video data, generated by OPD's RMC systems are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Description of the Technology

OPD uses different RMC systems to observe and/or record activity to promote public safety. Some RMCs allow for real-time remote access viewing of activity captured by the RMC lens. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Mobile functionality as well as battery power allows RMCs to be moved and positioned as the need requires.

A – 1. How Remote and Mobile Cameras (RMC) Work

Some RMCs are standard consumer-type cameras that can be held and operated by personnel. RMCs may also be affixed to a variable lens's for different views. RMCs can be attached to a camera monopod and used like a standard digital video camera; the monopod in this case extends the cameras perspective beyond arms reach so that personnel extend the range of view (beyond corners, above head-level in a crowd, or in other related situations). RMCs attached to monopods/tripods provide greater viewing access and promote safety where personnel may need to exercise caution before moving into unknown situations. RMCs may also be attached to utility poles for real-time and long-term remote viewing. In such cases RMCs may be powered through electricity of the utility pole or via portable battery power. In either case, RMCs offer personnel critical situational and evidentiary information in a safe way.

RMCs may also be connected to portable devices that stream live audio and video to remote locations. Such devices provide critical situational and evidentiary information during large-scale mass events.

A – 2. RMC Systems

RMCs can be self-contained devices that record audio and video, which either:

1) store data onto an internal storage device; or 2) transmit data in real-time through various digital transmission formats.

1. RMCs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.
2. RMCs can be mounted to telescoping monopods to simply extend the range of a RMC. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.
3. RMCs may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use RMCs or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use RMC equipment, software or data for any unauthorized purpose.

2. No member of this department shall operate RMC equipment or access the internally stored RMC data without first completing department-approved training.

3. The RMC systems shall only be used for official law enforcement purposes.

4. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Information Technology Unit and Criminal Investigations Division (CID) investigators, Internal Affairs Division personnel, crime analysts, the Office of the District Attorney) will have access to RMC audio and video data and system applications.

5. Accessing data collected by RMC systems requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an criminal or administrative investigation.

C. RMC Data

C – 1. Data Collection and Retention

RMC system data is maintained both by currently maintained by either: 1) the OPD Information Technology (IT) Unit within in the Bureau of Services (BOS); or 2) by the Intel Unit. Personnel using RMCs from the Intel Unit shall return RMCs at the end of their shift. The Intel Unit RMC Coordinator shall download the data onto secure Intel Unit computers within 24 hours of receiving returned RMC equipment.

The Intel Unit shall maintain all RMC data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an investigation. The OPD Unit and/or assigned personnel issued the RMC is responsible for recovering the data from the RMC.

Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.

The Intel Unit shall delete all RMC data left on installed on Intel Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

C – 2. Data Security

All RMC data will be closely safeguarded and protected by both procedural and technological means:

1. All RMCs shall be housed and secured within IT Unit or Intel Unit lockers. All RMC data downloaded from RMCs shall be uploaded onto secure user and email password protected IT Unit computers and / or Intel Unit computers.
2. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Those are the protocols used PEU or IAD or RMM systems.

3. Members approved to access RMCs under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training purposes.

C – 3. Releasing or Sharing RMC System Data

RMC system data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the RMC data that includes:

   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. RMC System Administration

OPD's RMC system oversight as well as data retention and access, shall be managed by OPD's Information Technology Unit under the BOS, or designee.

D – 1. RMC System Coordinator

The title of the official custodian of RMC System Coordinator is …..

D – 2. RMC System Administrator

The RMC System Coordinator shall administer all RMC systems, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The RMC System Coordinator, or designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The RMC System Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of RMC system data.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of the RMC system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The RMC System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of times a RMC was deployed, and type of deployment.
2. The number of times RMC data was used as part of an investigation.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the Shotspotter system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees authorized to use the GLD system include completion of training by the GLD System Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed: